构建安全可靠的企业信息安全系统

网路神警上网行为监管系统

技术白皮书

北京盛世光明软件技术有限公司

2011 年 1 月

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

北京盛世光明软件技术有限公司在编写本文档时已尽最大努力保证其内容准确可靠，但北京盛世光明软件技术有限公司不对文档中的遗漏、不准确或错误导致的损失和损害承担任何责任。

联系方式

全国服务热线：400-6789-518

邮箱：services_ssgm@126.com

目 录

一、背景 4

二、网路神警上网行为监管系统 6

三、产品功能简介 7

3.1 监控上网行为 7
3.2 限制上网行为 8
3.3 记录存储工具拷贝内容 8
3.4 高性能过滤 8
3.5 日志查询 9
3.6 多级管理 10
3.7 资源管理 10
3.8 黑名单 11
3.9 临时组 11
3.10 绑定 MAC 地址 11
3.11 发送即时消息 11
3.12 操作日志 12
3.13 统计和分析功能 12

四、产品部署 13

4.1 网路神警上网行为监管系统部署方式 13
4.2 多级管理部署方式 15

五、产品技术特色 16

六、产品规格 17

6.1 硬件设备 17
6.2 支持软件 17

七、关于我们 18

一、背景

随着互联网技术和应用的快速发展，人们对互联网的认识和使用已越来越深入，据中国互联网中心 CNNIC 统计，截止到 2007 年 6 月 30 日，我国的网民总数为 16200 万人，并仍在以惊人的速度快速增长。但由于互联网的开放性及网上信息良莠不齐，使得网上各种不良信息也随之泛滥，特别是反动、色情、暴力等有害信息极大地危害着社会的稳定。而法轮功邪教组织、民运分子、各种敌对势力也利用这一舞台，对我国进行各种宣传攻势和渗透演变。

随着网络技术的飞速发展，各种网络应用日趋普及，上网的环境和方式也更加多样。网吧、单位、小区、酒店等各种公共上网场所的互联网应用已成为社会文化生活的一个部分。也正因如此，网络的安全性越来越引起广泛的关注。

就企业而言，互联网的飞速发展，给企业带来了丰富的信息资源，使企业能充分享受互联网带来的种种便利，大大增强了企业的竞争力，但与此同时，企业又面临经营成本提高、工作效率下降、管理混乱等新问题的困扰：在繁忙的工作时间里，您的员工却在网上如痴如醉地炒股票、精神百倍地聊天、聚精会神地浏览与工作无关的网站等。有关统计资料显示，上网人群中大约有三分之一上班时间是在网上浏览与学习无关的信息，包括网络在线游戏、网上炒股、网上看球赛和各种各样的网上论坛。公司的网络带宽未得到合理分配，主次未分，正常上网要求不能充分满足，极大地降低了工作效率。员工利用公司上网资源浏览色情、邪教、反动的网站，甚至有违法的网上行为，不仅使公司企业形象受损，甚至有可能给公司带来法律纠纷。当前企业管理者普遍面临的主要网络问题包括：

- 如何避免内部泄密

  随着互联网技术的发展，网络沟通手段多样化，如：FTP、E-Mail、TFTP、BBS、QQ、MSN、UC、POPO、SKYPE 等等，这些通讯手段方便了企业或个人间的交流和协作，但如果不能合理利用，必将成为企业信息泄密的工具和途径。内部机密资料外泄。传统的路由器、防火墙等网关设备无法对网络上传输的泄密信息或不良信息的内容进行深度分析，更无法记录到

传播信息时所使用的身份信息。企业很难做到对泄密信息的阻断，也无法获取维护自身权益所必要的手段和证据。因此，一种能够全面分析网络信息内容，并对企业机密信息能够进行过滤和记录的软件将成为企业管理人员维护自身权益，减少机密信息泄露或不良信息侵害的重要武器。

- 如何提高工作人员工作效率

企业互联网的接入一方面有效提高了企业的综合运营效率及市场竞争能力，但是，如果企业内部缺乏有效的网络管理措施时，自制力差、纪律性不强的企业员工难免会通过公司网络访问一些与工作无关的网站和一些网络应用、如网络聊天、网络炒股、网游、在线视频、在线交友、下载、新闻浏览等。这将极大影响工作人员的工作效率，最终导致整个企业工作效率低下，工作氛围恶化，严重背离企业接入互联网的初衷。企业依靠行政手段很难规范员工上网行为，效果差，还会因此代理高昂的用人成本。如果能利用特定的软件技术手段来实现这个效果，对企业决策者来说无疑是一个最佳的选择。

- 如何减少网络带宽的浪费

企业网络是企业通讯的基础，是保障企业正常通讯的支撑体系。在这个基础职场运行着企业各种管理系统，如 ERP 系统，CRM 系统，WEB，E-Mail 等，同时还运营着其他的各种各样的网络应用。据统计，在未对网络应用及流量进行有效管控的企业网络中，70%以上的网络流量被网络下载，网络视频，网络音频等占用。这样的网络使用状况，很难为企业的正常通讯提供保障，迫使企业为此而不断增加网络出口带宽，但是问题往往是无法解决的。为了保证企业正常的业务开展，减少网络开支，企业迫切需要一套能够对网络带宽进行有效管控的软件系统。

- 如何满足国家关于互联网的法律法规要求。

开放虚拟的互联网环境为人们提供了畅所欲言、相互交流、表达情感的场所，但一些不法分

子或道德沦丧者却利用互联网作为蛊惑人心，散发反动言论，传播有害信息、恶意诋毁或污蔑他人的工具。为了加强和规范对互联网接入行为的控制和管理，国务院和公安部相继发布了《互联网信息服务管理办法》、《计算机信息网路国际互联网安全保护管理办法》、《互联网安全保护技术措施规定》（即公安部 82 号令）等法律法规。国家明文要求所有接入互联网的单位或企业其网络接入条件必须严格遵守并符合以上由国家制定的信息安全管理法律法规的要求。因此，企业管理者迫切需要一种能够为其过滤敏感内容并提供上网信息记录和反查的软件系统，帮助其企业规避由网络接入所带来的法律风险。

综上所述，互联网作为新文化，它给人们带来了资源和便利，也带来了糟粕和荒废时间的工具。在充分发挥互联网作用的同时，应该减少其带来的不利因素。

北京盛世光明软件技术有限公司自主研发的网路神警上网行为监管系统将有效的解决以上问题。

二、网路神警上网行为监管系统

网路神警上网行为监管系统（以下简称网路神警）是针对所有与 Internet 相连的局域网开发设计的，能够提供强大的上网行为管理功能。通过从网址、IP 地址、关键词等方面设置过滤规则，可以实现对访问网址的限制功能。IP 访问限制，E-Mail 内容记录，BBS 发帖记录，网络聊天内容记录，屏幕记录，USB 存储设备拷贝记录，应用程序禁用等。

网路神警的功能模块一目了然，操作简单，不需要掌握任何计算机知识，也不需要经过任何培训，管理员只要点击几下鼠标，就可以完全实现对任意控制项目的控制。

网路神警由“网路神警上网行为监管系统”和“客户端”以及网路神警上网行为监管分控中心（局域网内远程控制系统）三个程序组成。网路神警分控中心实现了对运行网路神警的服务器的远程控制，可以远程进行设置及查询等工作。在服务器安装完“网路神警上网行为监管系统”后，在与服务器位于同一个局域网内的任何一台计算机上安装“网路神警分控中心”即可。针对部分功能网络神警上网行为监管系统可以采取强制安装客户端的措施，如 QQ 聊天记录，MSN 聊天记录，屏幕记录，USB

存储设备拷贝，禁用程序等功能需要安装客户端软件。

三、产品功能简介

3.1 监控上网行为

3.1.1 监控访问网站信息

监控界面显示选择受监控计算机的实时访问网站的信息，受到重点监控的计算机的浏览网页的信息总是显示在监控界面中。信息包括访问的网址、访问者、访问时间、是否被阻止等。如果禁止用户访问某个网址，用户访问时会提示无法访问。并且访问信息显示为醒目的红色。

3.1.2 监控聊天内容

用户可以根据自身的监控需要，选择监控聊天内容。系统会自动提示用户安装客户端。安装后，即可记录下用户的聊天内容。可以记录下聊天的计算机名称、IP 地址、聊天工具、聊天人和记录时间等信息，并且双击记录后，能够显示聊天或发帖的具体内容。

3.1.3 监控发帖内容

用户可以根据自身的监控需要，选择监控发帖内容，包括 web 邮件内容。系统会自动提示用户安装客户端。安装后，即可记录下用户的发帖内容。可以记录下发帖的计算机名称、IP 地址、MAC 地址和发帖时间等信息，并且双击记录后，能够显示发帖的具体内容。

3.1.4 监控桌面

网路神警支持远程查看桌面，管理员可以查看局域网内任何一个计算机的实时桌面，但是只能查看，不能对其进行控制。而且管理员还可以根据实际需要选择是否监控桌面。选中“桌面内容记录”后，即可抓拍桌面图片，还可以设置抓拍的时间间隔。

3.2 限制上网行为

3.2.1 限制访问流量

系统可以对受监控计算机的流量进行限制，设置其每一秒或者每一分钟或者每一小时的流量。如果用户的流量超过了设置的流量，通讯会自动阻断。

3.2.2 限制上网时间

系统可以实现对任何组和单机建立各种上网时间段限制。该时间段被禁止后，该组或单机的所有上网行为都将禁止，无论其他过滤规则是否允许。只需点击要禁止上网的时间段，即可实现分时段上网功能。

3.2.3 禁用任意程序

系统可以限制任何一个程序的运行，只需输入程序名称就可以。如禁用 QQ 聊天工具，只要输入 qq.exe 就可以了。

3.3 记录存储工具拷贝内容

能够记录移动存储介质，如移动硬盘的使用，拷贝文件详细内容等信息。

3.4 高性能过滤

3.4.1 网站过滤

系统可以实现对网站的过滤，管理员设置为禁止访问后，用户就无法访问。另外系统还提供了一个不良信息库，存放了一些非法网站信息。启动使用不良信息库后，用户将无法访问这些不良网站。不良信息库会定期及时更新。

3.4.2 关键词过滤

系统可以实现对关键词的过滤，管理员设置好为关键词后，用户就无法访问带有关键词的网页。

3.4.3 端口过滤

在网络中，端口就好比房子的门，数据要进出就必须通过这道门。网络中的服务都对应的某个或者某些端口，所以我们在对某些特定的特性服务就会使用到端口过滤了。比如像目前比较流行的 BT 等，它有个特征就是默认使用 6881~6889 端口。端口过滤通过禁用一些端口，禁止内部用户使用互联网上部分服务。

3.5 日志查询

系统可以查询受监控计算机上网的详细信息，包括上网日志、邮件、发帖日志、聊天内容、桌面抓拍和操作日志。为配合公安部第 82 号令的要求，系统默认的日志保留时间为 60 天，用户也可以根据实际需要设置 60 以上的其他时间。

3.5.1 查询范围设置灵活

计算机选择可以按照计算机名称、计算机 IP、计算机 MAC 地址、计算机分组的分类来选择；时间范围可以按照今天、本周、本月、本年、全部时间的分类来选择，也可以根据需要选择具体时间。

3.5.2 查询功能强大

可以查询任何计算机或计算机分组在任何时间的上网日志记录，还可以查询浏览某个具体网址或者 IP 地址的计算机信息。只需输入某个具体的网址，即可查询访问过该网址的所有计算机的记录。

3.5.3 查询结果详细

能够查询到访问的网址、访问的 IP 地址、访问时间和访问该网址的机器的名称、IP 地址和 MAC 地址的详细信息。

3.5.4 查询结果保存简便

方便实用的日志导出功能,使管理员可将监控日志导出做统一存储或分析。所有日志文件可存为EXCEL 文件，且都可打印输出。

3.6 多级管理

局域网内安装网路神警后，通过添加上级管理单位，该局域网可以接受上级单位的管理，从而执行上级单位发送的指令。一个本地服务器可以有多个上级服务器，当一个本地服务器接受多个上级管理时先接受优先级别高的上级的管理。上级单位的管理优先级分为：低优先级、中低优先级、中高优先级、高优先级。该功能的实现只需输入上级管理单位的名称、IP 地址和端口号等基本信息即可。

3.7 资源管理

3.7.1 分组管理

系统会自动搜索局域网内的计算机，搜索到的计算机将显示在“计算机列表”中，同时还会显示每台计算机名称、IP 地址、MAC 地址等内容。管理员可以对每台机器的名称进行修改如统一使用实名，以方便对系统进行统一管理。

用户对局域网内的计算机会有不同的监控要求，为此网路神警系统设置了四个分组，分别是监控组、黑名单、临时组和未授权。

对于不同的分组网路神警进行不同的管理，对监控组内的计算机会根据用户设置的监控要求进行一定的上网行为限制，如上网时间限制、禁止聊天限制、禁止访问某些网页等；

当计算机数量超出授权数量时，系统自动将超出数量的计算机加入未授权分组中。进入未授权分组中的计算机在试用版时不做任何监控处理，注册为正式版之后，将无法上网。

3.7.2 多级分组管理

网路神警系统能够根据用户实际采用的组织结构对局域网内的计算机进行分组，以实现针对不同的部门进行不同的上网行为控制。如企业用户可以添加研发部、销售部、财务部等分组，研发部还可以分为研发 1 组和研发 2 组；学校用户可以添加教务处、学生处等分组。

3.8 黑名单

对于局域网内存在恶意行为的计算机可以将其放入黑名单，进行完全封杀，限制其所有上网行为。

3.9 临时组

网路神警运行期间，系统会定时搜索局域网内的计算机，并将新搜索的计算机添加到临时组。对于临时组中的计算机服务器只记录其上网日志，并不对其上网行为进行控制。临时组中的电脑可以设置为允许上网或者禁止上网，用户可以根据单位的实际情况设置。

3.10 绑定 MAC 地址

用户可以根据实际需要，设置 IP 与 MAC 地址是否绑定。将某个计算机设置为 IP 地址和 MAC 地址绑定，如果该机器更改 IP 地址，则无法上网。这样可以防止局域网内的计算机用户随意更改 IP 地址。

3.11 发送即时消息

网路神警支持发送即时消息功能，管理员可以向受到监控的任何一台计算机发送即消息，对其进行提醒。例如某企业用户，管理员查看到某个员工在上班时间玩游戏，就可 以给他发送消息“请上班时间不要玩游戏”。

3.12 操作日志

网路神警系统能够详细记录系统管理员的登录、用户管理、分组管理等日志。记录内容详细，操作时间、操作用户、被操作计算机的 IP、被操作计算机的名称、被操作计算机的 MAC、操作内容、操作是否成等都可以记录。

3.13 统计和分析功能

统计网站排名

可以显示局域网内某个计算机或某些计算机在某个时间范围访问网站的次数，时间范围可以随意设置。可以分别选择网站被点击排名和终端点击排行来查看。查询结果按访问次数的多少进行排列

统计在线时间

可以查询某个计算机或某些计算机的在某个时间范围访问外网时间，时间范围可以随意设置。查询结果按在线时间长短排序。

统计实时流量

查看局域网内计算机流量信息。可以选择要查询的流量类型：上传和下载总流量、上传流量、下载流量。点击“统计”后下方显示查询结果，流量单位为：knps。查询结果可以保存 Excel 表格中。

统计资源

统计在局域网内的各种资源的数量，包括授权终端数量、授权分控数量、实际终端数量、在线终端数量。其中授权终端数量和授权分控数量由按照购买软件时授权的数量确定；实际终端数量是按照曾经接入本局域网的电脑终端的累计数量确定。基本上等于本系统内注册的 MAC 地址的数量；在线终端数量是查询当时那一刻实际在线的终端电脑的数量。

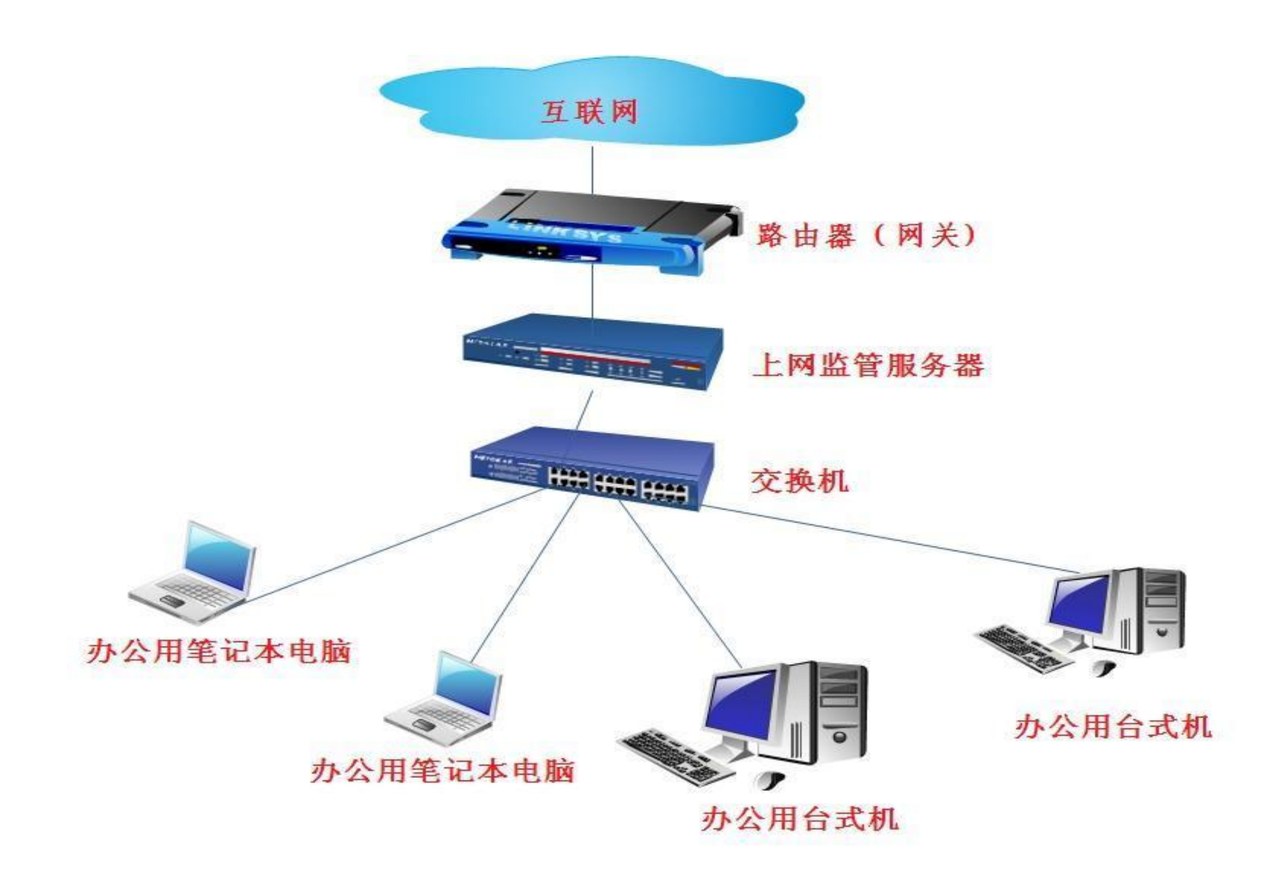
四、产品部署

网路神警上网行为监管系统部署方式分为上网行为监管部署和多级管理部署方式 2 类，网路神警上网行为监管系统主要支持桥接和旁路监听 2 种工作模式，能够充分满足组网环境及其管理需求。每一种工作模式均具有其相应特点和优势。现做如下介绍。

4.1 网路神警上网行为监管系统部署方式

桥接模式

网桥模式的部署方式是将网路神警上网行为监管系统串接到网关设备（网络出口）与内部核心交换机之间，该部署模式一般不需要改变其网络环境和原有设备的配置。由于是串接的网络中，所有到达外部网络的数据流必须经过该设备。因此，桥接模式可以对网络中的应用进行控制，对流量进行审计、对内容进行过滤和审计等，还可以强制推送客户端到被控端桌面。，桥接模式适合不想改变原有网络结构，但是系统通过该系统能够实现应用控制和审计的场合。



旁路监听模式

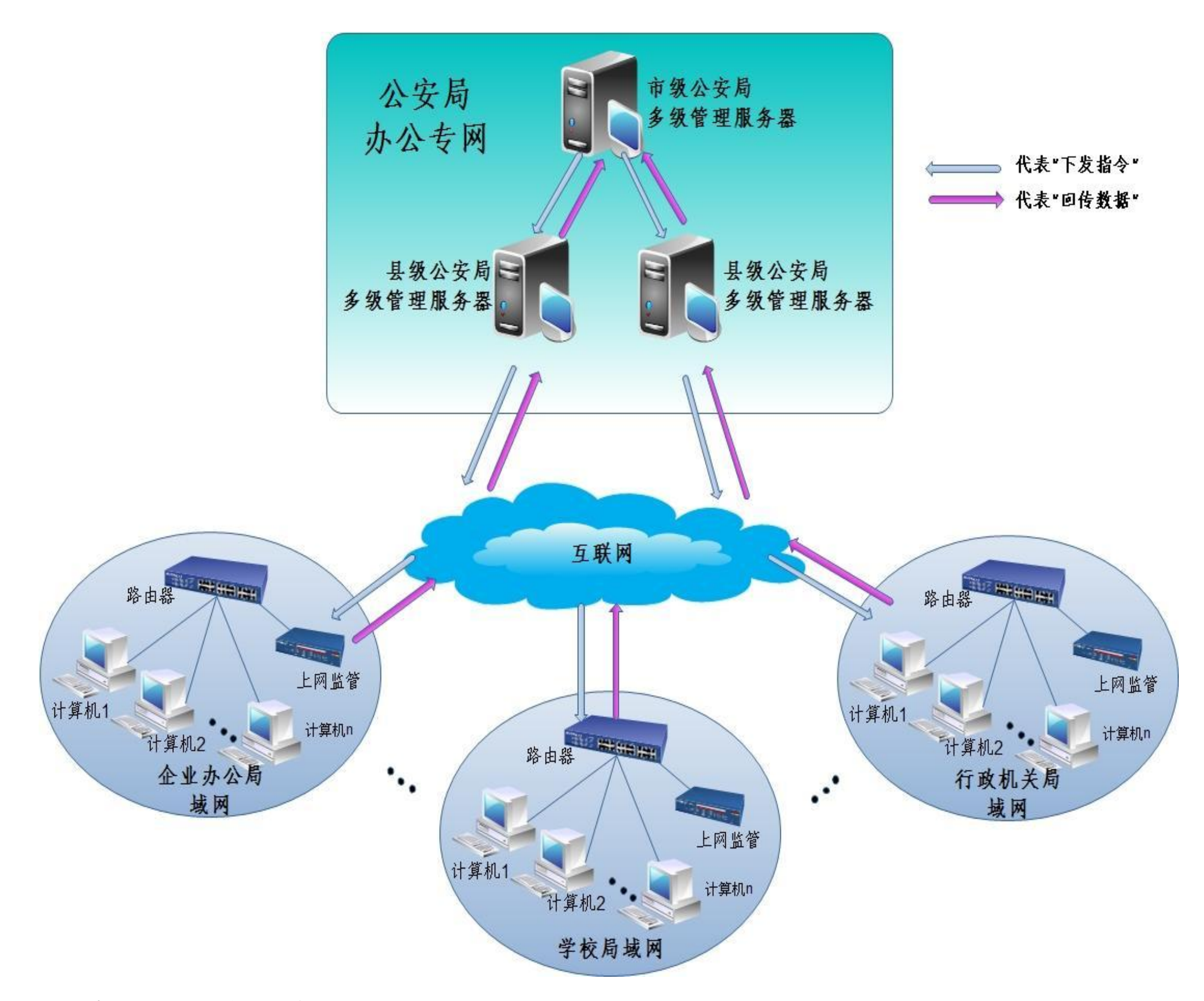
旁路监听模式的部署方式是将网路神警上网行为监管系统部署在网络核心交换上，并打开核心交换机的端口镜像功能，对其进行合理的配置，通过镜像端口将网络数据流输出到网路神警上网行为监管系统上，以实现对网络数据的审计功能。旁路监听模式能实现桥接模式的所有功能，由于是非串接模式，因此最大的好处是如果上网行为监管系统出现故障不会影响原有网络的正常运行。该模式适合于对网络稳定性要求非常高，只希望对网络应用，流量进行审计，不需要控制的场合。



4.2 多级管理部署方式

多级管理需要部署在上级管理部门的机房中，核心作用是集中管理、指令下发、数据回传、统计查询，可以实现上级对下级网站服务器的集中管理，对全部联网单位的统一管理。利用多级管理系统来协调各县市区以及乡镇的管理工作，能够及时准确地发现网站中的非法内容并做出阻断传输的处理。市级管理服务器可以设置报警指令、过滤指令和查询指令等指令，使县区的服务器接受市级管理服务器的管理，无条件执行市级管理服务器的指令，这样市级管理部门就可以轻松掌握基层服务器的内容并对内容做出监管。

网络拓扑图如下：



五、产品技术特色

1. 部署方便，内置网桥工作模式，即插即监控；或配合使用固化路由器，只需要接入该固化路由器的固化镜像端口就能够实现监控。

2. 策略灵活，对被监控计算机进行分组管理，可以对不同分组设置不同的过滤规则。

3. 多级管理模式 对下级监控单位实施分级集中管理，统一设置过滤规则；支持数据回传。符合 GA 659-2006， GA 660-2006，GA 661-2006，GA 663-2006 等行业标准，能够与现有公安内部管理系统能可靠对接

4. 分控中心功能，局域网内任何一台安装有分控中心的计算机被授权后，登录监控服务器对其他上网的计算机客户端进行临时控制的监控。

5. 重点监控功能，可以设置需要重点监控的计算机，随时即时重点筛选查看其上网状况。

6. 虚拟身份采集，网上使用的即时通讯工具账号（如 QQ 号码、MSN 账号等）、电子邮箱、游戏账

号及在网站交互式栏目注册的用户名称等均可在网站后台进行采集。

7. 强制安装客户端并自动分发，安装客户端后能实现桌面监控和聊天内容监控等功能，系统可以设置强制安装客户端，不装客户端就无法上网并提示下载安装客户端，被监控计算机可以自行下载安装。解决了手动安装客户端的麻烦和客户端恶意破坏的弊端，大大减少管理员的管理成本。

六、产品规格

6.1 硬件设备

监控服务器配置最低要求：

1）50 台以下： CPU P42.8，内存 512M,硬盘 40G(最低 10G 剩余空间)。

2）100 台以下：CPU P42.8，内存 1G，硬盘 40G（最低 15G 剩余空间）。

3）100 台以上：CPU P43.0，内存 1.5G 硬盘 80G（最低 20G 剩余空间）。

客户端要求：

按要求网络拓扑接入局域网即可。

6.2 支持软件

适用操作系统：Windows 2000 Server/Windows XP/Windows 2003

推荐操作系统：Windows 2000 Server

数据库：支持 MySQL 和 MS SQL2000 两种

七、关于我们

北京盛世光明软件技术有限公司是一家专业从事软件技术开发、软件产品生产、网站运营、电子商务的高科技公司，位于国家软件产业基地、国家软件出口基地的中关村软件园，是软件园区的一颗璀璨明星，中国软件协会成员单位、北京科委认定高新技术企业、双软企业。在济宁设立了研发基地，并成立济宁盛世光明软件技术有限公司，公司拥有一支富有创新、开拓精神的高素质的战斗团队，济宁盛世光明软件是北京盛世光明软件具备国内一流的软件开发技术和工程施工技术水平。为客户提供最佳的解决方案和专业化的服务。

★公司宗旨：致力于国家计算机网络信息安全的保护；坚持以人为本，走科技创新之路，发展拥有自主知识产权的国际领先的信息安全技术支撑体系；获得领先的市场销售地位、不断增长的利润和价值，从而令我们的员工、股东以及我们生活和工作所处的社会共同繁荣。

★软件研发中心：公司拥有自主知识产权的四大软件产品系列：网路神警上网行为监管软件、互联网信息安全审计系统、网路神警家庭小卫士和盛世光明教育信息化建设管理平台系统；其中网路神警上网行为监管系统 2007 年获得北京市科技创新奖，并且已通过公安部检测认证，获得公安部颁发产品销售许可，目前已经在国内市场广泛应用，并得到了用户的好评。

★市场拓展中心：针对公司自主知识产权的产品，通过行业客户群体的定向联系、全国代理商体系的建立、国际互联网网络宣传等形式全面拓展全国市场，提高市场占有率和市场普及率。

★科技创新中心：对比同行业产品优势，收集反馈意见和建议，对产品、技术和市场发展进行前瞻性研究，不断提高公司科技创新的水平。

★客户服务中心：利用一切现代化的技术手段，通过网站技术支撑平台、400 免费电话、EMAIL 及网络在线交流、电话指导、远程在线技术协助、现场服务等方式，为客户提供尽善尽美的服务支持，全面提升公司的服务水平。

★主营业务：计算机软件开发、网络安全服务。公司自主研发的产品主要面向网络信息安全服务领域。

网站连接：http://www.ssgm.net

全国统一销售服务热线：400-6789-518

总部地址：北京市海淀区信息路甲 28 号科实大厦 A 座 A4-3A (邮编：100193)

山东基地：山东省济宁市高新开发区金宇路 54 号（邮编：272000）